Основы Информационной Безопасности

Онлайн лекция 05.02.2018

Лектор: Доцент кафедры ОЗиБЖ Кабиров Т.Р.

БГПУ им. М.Акмуллы

Рассматриваемые вопросы

- Что такое информация?
- Виды и свойства информации
- Понятие информационной безопасности и ее задачи
- Эволюция информационных взаимоотношений
- Конфиденциальная информация и ее защита
- Классификация информационных угроз
- Методы и средства защиты информации
- Информационно-психологические угрозы

Литература

- Артемов, А.В. Информационная безопасность : курс лекций / А.В. Артемов ; Межрегиональная академия безопасности и выживания. - Орел : МАБИВ, 2014
- Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015
- Журавленко, Н. И. Информационная безопасность и защита от информационного воздействия: учеб. пособие - Уфа : [БГПУ], 2010
- Гафнер В.В. Информационная безопасность: учеб. пособие: Феникс, 2010. – 324 с.
- Днепров А.Г. Защита детей от компьютерных опасностей 2008. – 192 с.
- Загородников С.Н. Основы информационного права: уч. пособие для студ. ВУЗов, 2005. -195с.
- Петров В.П. Информационная безопасность человека и общества: уч. Пособие 2007. – 336 с.

Информация - это всеобщее свойство материи

Любое взаимодействие в природе и обществе основано на информации

Всякий процесс совершения работы есть процесс информационного взаимодействия

Информация - продукт отражения действительности

Действительность отражается в пространстве и времени

Ничего не происходит из ничего

Информация сохраняет свое значение в неизменном виде до тех пор, пока остается в неизменном виде носитель информации

«информация» происходит от латинского слова «***informatio***», что означает *сведения, разъяснения, изложение.*

«информация – *это общенаучное понятие, включающее обмен сведениями между людьми, человеком и автоматом, автоматом и автоматом, обмен сигналами в животном и растительном мире; передачу признаков от клетки к клетке, от организма к организму***».**

«информация – *сведения (сообщения, данные) независимо от формы их представления».*

Информация - сведения об объектах и явлениях окружающей среды, их параметрах, свойствах и состоянии, которые воспринимают информационные системы (живые организмы, управляющие машины и др.) в процессе жизнедеятельности и работы.

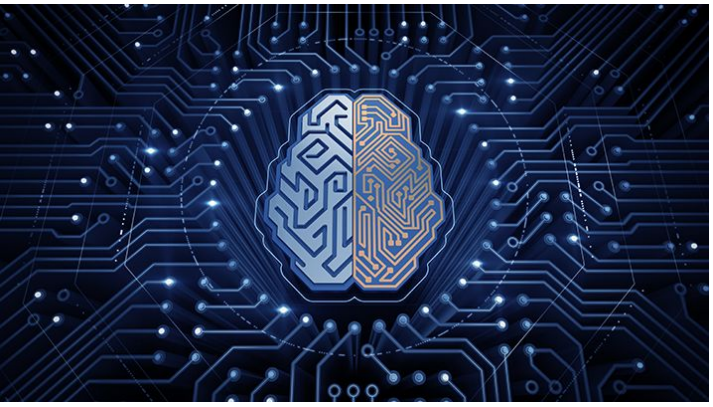
Данные - фиксируемые в виде определенных сигналов воспринимаемые факты окружающего мира.

Данные несут в себе сведения о событиях, произошедших в материальном мире, и являются регистрацией сигналов, возникших в результате этих событий. Однако данные не тождественны информации. Станут ли данные информацией – зависит от того, известен ли метод преобразования данных в известные понятия.

Знание - *форма существования и систематизации результатов познавательной деятельности человека*

Знание в широком смысле — субъективный образ реальности в форме понятий и представлений

Информацию человек может получать откуда угодно, а знания приходят тогда, когда человек использует эту информацию и сочетает ее со своим собственным опытом. Информация становится знанием, когда она переработана и проанализирована человеческим мозгом. Знание существует только благодаря людям. Знание - это осознание, понимание и толкование определенной информации с учетом путей наилучшего ее использования для достижения конкретных целей



фиксируемые воспринимаемые факты окружающего мира представляют собой **данные.**

При использовании данных в процессе решения конкретных задач появляется **информация**.

Результаты решения задач, истинная, проверенная информация (сведения), обобщенная в виде законов, теорий, совокупностей взглядов и понятий представляют собой **знания.**

Виды и свойства информации

Виды и свойства информации

По форме представления

- Буквенная
- Цифровая
- Графическая
- Кодированная
- Комбинированная

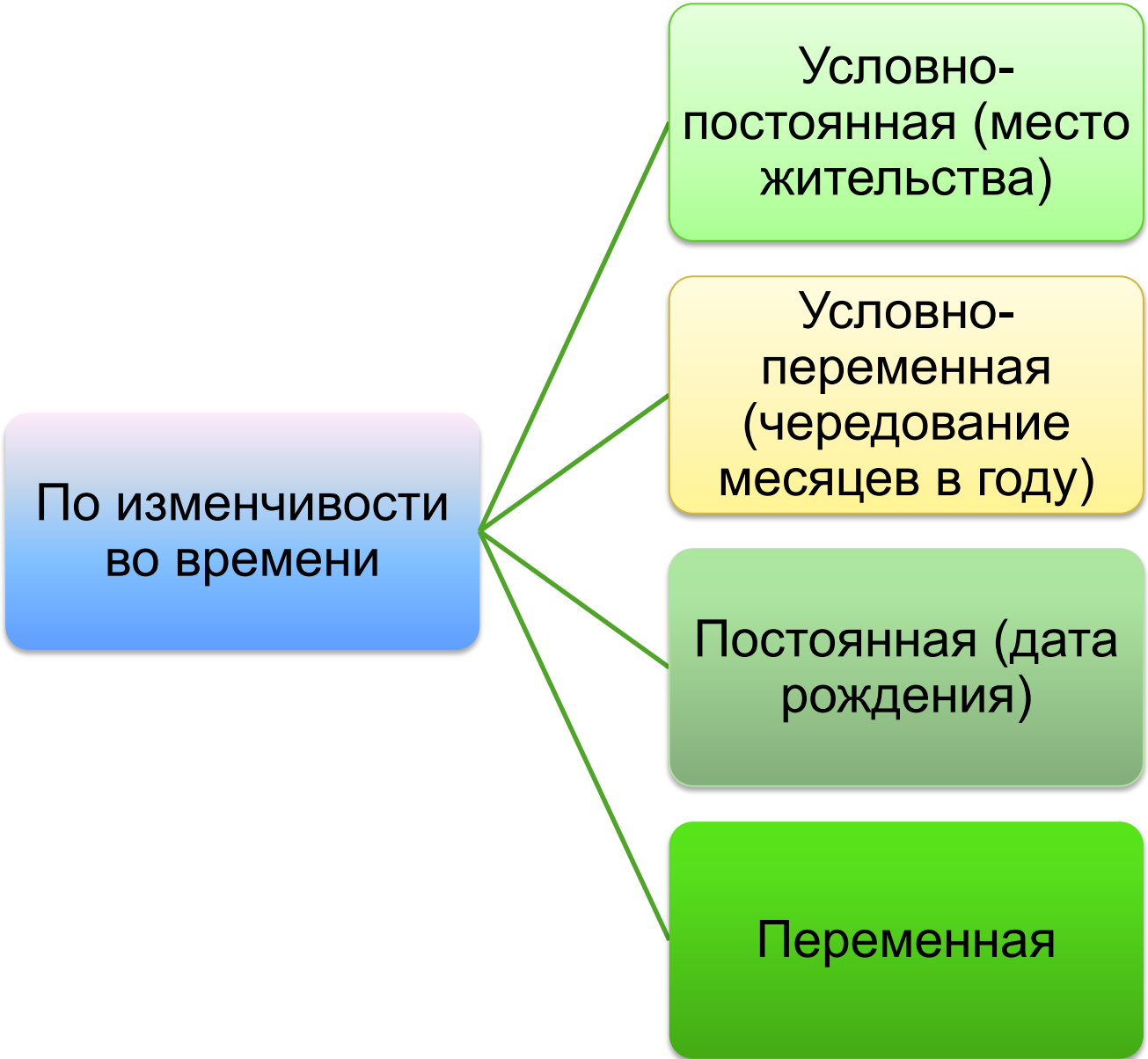
По форме передачи

- Вербальная
- Невербальная
- Письменная
- Печатная
- Телефонная
- Электронная и др.

По назначению

- Экономическая
- Техническая
- Социальная
- Организационная
- другие

Виды и свойства информации



Виды и свойства информации

Как и всякий объект, информация обладает **свойствами.**

Информация отличается от других объектов природы и общества характерной особенностью: на свойства информации влияют как **свойства исходных данных, составляющих ее содержательную часть**, так и **свойства методов, фиксирующих эту информацию**.

1. Атрибутивные свойства - свойства, без которых информация не существует.

2. Прагматические свойства - свойства, которые характеризуют степень полезности информации для пользователя, потребителя и практики.

3. Динамические свойства - свойства, которые характеризуют изменение информации во времени.

Структура информационного процесса

Те предметы или устройства, от которых человек может получить информацию, называют **источниками информации**

Те предметы или устройства, которые могут получать информацию, называют **приёмниками информации.**

Передача - перенос информации в виде сигнала в пространстве посредством физических сред любой природы.

Обработка - любое преобразование информации с целью решения определенных функциональных задач (они определяются потребителем информации). Данная фаза может включать хранение информации как перенос ее во времени.

Понятие информационной безопасности

Информационная безопасность - защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб владельцам или пользователям информации и поддерживающей инфраструктуры.

Защита информации - *деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния.*

Международный день защиты информации отмечается 30 ноября с 1988 года. В этот год произошла первая массовая компьютерная эпидемия - эпидемия червя Морриса.

Объектом ИБ будет считаться *информация, затрагивающая государственные, служебные, коммерческие, интеллектуальные и личностные интересы, а также средства и инфраструктура её обработки и передачи.*

Субъектами ИБ *являются* органы и структуры, которые в той или иной мере занимаются ее обеспечением

Кроме этого, субъектами ИБ могут быть:
граждане и общественные объединения;
средства массовой информации;
предприятия и организации независимо от формы собственности.

Цель мероприятий в области информационной безопасности - защита интересов субъектов ИБ.

Задачи ИБ:

- Обеспечение права личности и общества на получение информации.
- Обеспечение объективной информацией.
- Борьба с криминальными угрозами в сфере информационных и телекоммуникационных систем, с телефонным терроризмом, отмыванием денег и т.д.
- Защита личности, организации, общества и государства от информационно-психологических угроз.
- Формирование имиджа, борьба с клеветой, слухами, дезинформацией.

Информационные опасности и угрозы

Источниками **внутренних** угроз являются:

- Сотрудники организации.
- Программное обеспечение.
- Аппаратные средства.

Внутренние угрозы могут проявляться в следующих формах:

- ошибки пользователей и системных администраторов;
- нарушения сотрудниками фирмы установленных регламентов сбора, обработки, передачи и уничтожения информации;
- ошибки в работе программного обеспечения;
- отказы и сбои в работе компьютерного оборудования.

Информационные опасности и угрозы

К **внешним** источникам угроз относятся:

- Компьютерные вирусы и вредоносные программы.
- Организации и отдельные лица.
- Стихийные бедствия.

Формами проявления внешних угроз являются:

- заражение компьютеров вирусами или вредоносными программами;
- несанкционированный доступ к корпоративной информации;
- информационный мониторинг со стороны конкурирующих структур, разведывательных и специальных служб;
- действия государственных структур и служб, сопровождающиеся сбором, модификацией, изъятием и уничтожением информации;
- аварии, пожары, техногенные катастрофы, стихийные бедствия.

Информационные опасности и угрозы

По способам воздействия на объекты информационной безопасности угрозы подлежат следующей классификации:

- информационные
- программные
- физические
- радиоэлектронные
- организационно-правовые.

Информационные опасности и угрозы

К **информационным** угрозам относятся:

- несанкционированный доступ к информационным ресурсам;
- незаконное копирование данных в информационных системах;
- хищение информации из библиотек, архивов, банков и баз данных;
- нарушение технологии обработки информации;
- противозаконный сбор и использование информации;
- использование информационного оружия.

Информационные опасности и угрозы

К **программным** угрозам относятся:

- использование ошибок и «дыр» в программном обеспечении;
- компьютерные вирусы и вредоносные программы;
- установка «закладных» устройств.

К **физическим** угрозам относятся:

- уничтожение или разрушение средств обработки информации и связи;
- хищение носителей информации;
- хищение программных или аппаратных ключей и средств криптографической защиты данных;
- воздействие на персонал.

Информационные опасности и угрозы

К **радиоэлектронным** угрозам относятся:

- внедрение электронных устройств перехвата информации в технические средства и помещения;
- перехват, расшифровка, подмена и уничтожение информации в каналах связи.

К **организационно-правовым** угрозам относятся:

- нарушение требований законодательства и задержка в принятии необходимых нормативно-правовых решений в информационной сфере;
- закупки несовершенных или устаревших информационных технологий и средств информатизации.

Информационные опасности и угрозы

Информатизация - организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного само-управления, организаций, общественных объединений на основе формирования и использования информационных ресурсов.

Роль информации в развитии общества

Технологическая революция - радикальное изменение доминирующего в обществе технологического уклада, который, в свою очередь, определяется средствами и способами организации общественного производства и жизнеобеспечения общества.

Информационная революция - это преобразование общественных отношений из-за кардинальных изменений в сфере обработки информации

Первая информационная революция (устная) заключается в появлении языка и членораздельной человеческой речи.

Вторая революция (письменная) связана с изобретением письменности.

Третья информационная революция (печатная) была вызвана изобретением печатного станка.

Четвертая информационная революция (электронная) началась в XIX веке и была обусловлена изобретением электричества, благодаря которому появились телеграф, телефон, радио, телевидение.

Пятая информационная революция (компьютерная) началась в 50-е годы XX века с появлением средств цифровой вычислительной техники.

Шестой информационной революцией (сетевой) стало объединение компьютеров для передачи данных в сети, что привело к появлению единого глобального информационного пространства. Некоторые специалисты ставят появление Интернета по его влиянию на цивилизацию в один ряд с книгопечатанием.

Интернет - открытая, саморазвивающаяся кибернетическая система, включающая в себя миллионы компьютеров, объединённых в различные локальные и глобальные сети

Информационная технология - это представленное в пригодном для практического использования виде концентрированное выражение научных знаний и практического опыта, позволяющее рациональным образом организовать тот или иной достаточно часто повторяющийся информационный процесс

По расчетам, приведенным Л. Д. Рейманом, пятьдесят лет тому назад, пересылка по почте 30 страниц текста на расстояние 5 тысяч километров длилась бы примерно 10 дней и стоила бы около 30 долларов. Двадцать лет назад, используя факс, подобная пересылка заняла бы примерно 1 час, и стоимость составляла около 50 долларов. Сегодня на это требуется не более секунды, а стоимость составит около 3 центов. Таким образом, стоимость упала в 1000 раз, скорость возросла в 300 тысяч раз.

По подсчётам ученых, с начала нашей эры для удвоения знаний потребовалось 1750 лет, второе удвоение произошло в 1900 году, третье - в 1950 году и так далее в геометрической прогрессии. Быстрое сокращение времени удвоения объёма накопленных научных знаний указывает на явление, получившее название «информационный взрыв» и свидетельствующее о начале века информации, возникновении информационного общества.

Информационное общество - это ступень развития цивилизации, в которой главными продуктами производства являются информация и знания.

Ноосфера - сфера взаимодействия общества и природы, в границах которой разумная человеческая деятельность становится определяющим фактором развития.

"Человечество … становится мощной геологической силой. И перед ним, перед его мыслью и трудом, становится вопрос о перестройке биосферы в интересах свободно мыслящего человечества как единого целого. Это новое состояние биосферы, к которому мы, не замечая этого, приближаемся, и есть ноосфера… [Человек] может и должен перестраивать своим трудом и мыслью область своей жизни, перестраивать коренным образом по сравнению с тем, что было раньше".

Владимир Иванович Вернадский

ОСНОВЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информация как объект правового регулирования

Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ Об информации, информационных технологиях и о защите информации

Ключевые принципы обеспечения информационной безопасности

Организация информационной безопасности предполагает разработку определённых **принципов** её обеспечения. Одним из основных является принцип **баланса интересов личности, общества и государства.**

Принцип **законности и правой обеспеченности**

Принцип **интеграции с международными системами безопасности информации.**

Принцип **экономической эффективности**

Принцип **усиления самого слабого звена**

В соответствии с ФЗ «Об информации, информационных технологиях и о защите информации» защите подлежат сведения ограниченного доступа, а степень защиты определяет их собственник.

Не может быть ограничен доступ к:

- нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;
- информации о состоянии окружающей среды;
- информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);
- информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;
- иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

Доктрина информационной безопасности РФ представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Информационная безопасность РФ - *это состояние защищённости её национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.*

Конфиденциальная информация и её защита

- *Коммерческая тайна.*
- *Служебная тайна.*
- *Профессиональные тайны.*
- *Государственная тайна.*

Коммерческая тайна

Коммерческая (служебная) тайна *негосударственной организации* - сведения, не являющиеся государственными секретами, которые связаны с производственной, управленческой, финансовой или иной деятельностью организации и распространение которых может нанести ущерб её интересам.

Собственник коммерческой информации на основании совокупности перечисленных критериев определяет её ценность для своей хозяйственной деятельности и принимает соответствующее оперативное решение

Профессиональные тайны

В соответствии с действующим законодательством к профессиональной тайне относится информация, связанная со служебной деятельностью медицинских работников, нотариусов, адвокатов, частных детективов, священнослужителей, работников банков, ЗАГСов, учреждений страхования. В качестве субъекта профессиональной тайны может выступать как юридическое, так и физическое лицо.

Профессиональная тайна **-** информация, защита которой от несанкционированного распространения является обязанностью субъекта в силу выполняемых им профессиональных функций

Профессиональные тайны

банковская тайна. Понятие банковской тайны, в соответствии со ст. 857 ГК РФ, охватывает сведения о банковском счёте, вкладе, операциях по счёту, а также сведения о клиентах банка.

Банковская тайна защищает конфиденциальную информацию клиента или коммерческую информацию корреспондента.

Банк России не вправе разглашать сведения о счетах, вкладах, а также сведения о конкретных сделках и об операциях из отчетов кредитных организаций, полученные им в результате исполнения лицензионных, надзорных и контрольных функций, за исключением случаев, предусмотренных федеральными законами.

Профессиональные тайны

нотариальная тайна.

Тайна является специфическим правилом нотариальных действий. В соответствии со ст. 5 Основ законодательства РФ о нотариате нотариусу при исполнении служебных обязанностей, а также лицам, работающим в нотариальной конторе, запрещается разглашать сведения, оглашать документы, которые стали им известны в связи с совершением нотариальных действий, в том числе и после сложения полномочий или увольнения, за исключением случаев, предусмотренных Основами. Обязанность хранить профессиональную тайну включена в текст присяги нотариуса.

Профессиональные тайны

процессуальные тайны обычно делят на два вида:

- следственную тайну
- тайну совещания судей

Следственная тайна связана с интересами законного производства предварительного расследования по уголовным делам

Эта процедура имеет одной из целей запрет на разглашение информации о дискуссиях, суждениях, результатах голосования, которые имели место во время совещания судей.

Профессиональные тайны

врачебная тайна.

Согласно ст. 61 Основ законодательства РФ об охране здоровья граждан информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении, составляют врачебную тайну.

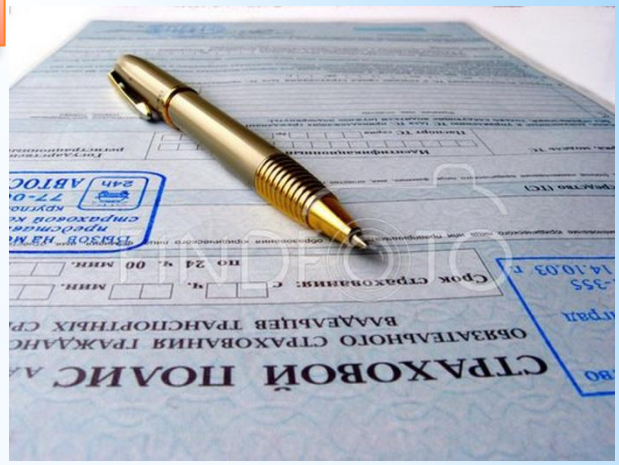
Гражданину должна быть подтверждена гарантия конфиденциальности передаваемых им сведений.

Профессиональные тайны

адвокатская тайна.

В соответствии с ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» адвокат, помощник адвоката и стажер адвоката не вправе разглашать сведения, сообщенные доверителем в связи с оказанием ему юридической помощи. Причем доверительные сведения, полученные адвокатом, могут быть как в виде документов, так и в устном виде. Законом установлены гарантии независимости адвоката. В частности, адвокат не может быть допрошен в качестве свидетеля об обстоятельствах, которые стали ему известны в связи с исполнением им обязанностей защитника или представителя

Профессиональные тайны



тайна страхования.

Институт страховой тайны во многих отношениях схож с институтом банковской тайны. Тайну страхования, в соответствии со ст. 946 ГК РФ, составляют полученные страховщиком в результате своей профессиональной деятельности сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц. За нарушение тайны страхования страховщик в зависимости от рода нарушенных прав и характера нарушения несет ответственность в соответствии с правилами, предусмотренными ст. 139 или ст. 150 ГК РФ.

Профессиональные тайны

тайна связи.

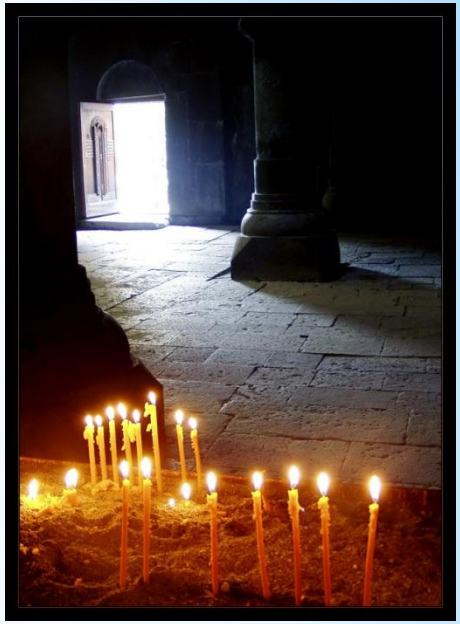
ФЗ «О связи» в части защиты информации регулирует общественные отношения, связанные с обеспечением невозможности противоправного ознакомления с сообщениями, передаваемыми любыми субъектами - физическими или юридическими лицами - по средствам связи. При такой постановке вопроса тайна связи становится инструментом обеспечения сохранности конфиденциальной информации.

Профессиональные тайны

тайна усыновления.

Институт тайны усыновления связан с интересами охраны семейной жизни и выражается в установлении гражданской и уголовной ответственности за разглашение тайны усыновления (удочерения). Согласно ст. 155 УК РФ тайна усыновления может быть двух разновидностей. Первой обладают лица, которые обязаны хранить факт усыновления как служебную или профессиональную тайну (судьи, работники местных администраций, органов опеки и попечительства и прочие лица, указанные в ч. 1 ст. 139 СК РФ). Второй - все другие лица, если установлены их корыстные или иные низменные побуждения при разглашении тайны усыновления без согласия обоих усыновителей.

Профессиональные тайны



тайна исповеди.

Обеспечение тайны исповеди является внутренним делом священника; юридической ответственности за её разглашение он не несет. Согласно ч. 2 ст. 51 Конституции РФ и ч. 7 ст. 3 ФЗ «О свободе совести и религиозных объединениях» священнослужитель не может быть привлечен к ответственности за отказ от дачи показаний по обстоятельствам, которые стали ему известны из исповеди.

Защита государственной тайны

Правовой институт государственной тайны имеет три составляющие:

- сведения, относимые к определенному типу тайны (а также принципы и критерии, по которым сведения классифицируются как тайна);
- режим секретности (конфиденциальности) - механизм ограничения доступа к указанным сведениям, т.е. механизм их защиты;
- санкции за неправомерное получение и (или) распространение этих сведений.

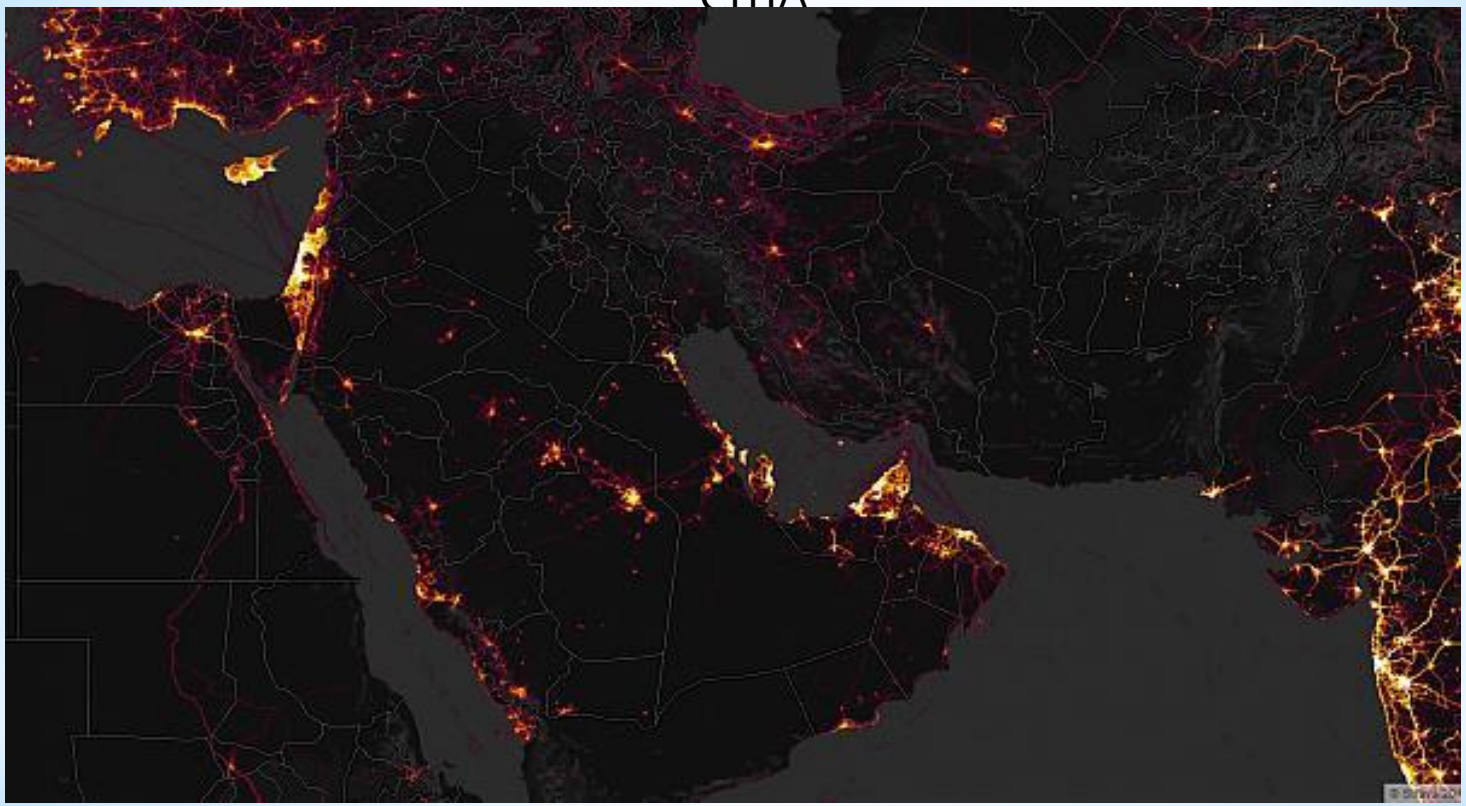
Государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

К сведениям **особой важности** относят такие сведения, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких областях.

К **совершенно секретным** сведениям относят такие сведения, распространение которых может нанести ущерб интересам министерства (ведомства) или отраслям экономики Российской Федерации в одной или нескольких областях.

К **секретным** сведениям относят все иные из числа сведений, составляющих государственную тайну. Ущерб может быть нанесен интересам предприятия, учреждения или организации.

Устройства для занятий спортом с приложением компании Strava позволили определить точное местоположение секретных военных баз США



Данные фитнес-трэкера из некоторых регионов мира, таких как страны Ближнего Востока, говорят о том, что в этих районах, по-видимому, расположены военные базы, персонал которых использует приложение во время тренировок. В зонах, где идут военные действия, персонал, использующий фитнес-трэкеры, - это, скорее всего, солдаты либо армии США, либо других западных стран

По материалам http://ru.euronews.com/

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Для защиты информации при помощи устройств применяются три основных класса контроля доступа. К ним относятся:

контроль, основанный на обладании (ключи);

контроль, основанный на личных характеристиках (биометрия)

контроль, основанный на знании (пароли)

Меры контроля доступа должны обеспечить две вещи. Во-первых, человек должен попасть в систему, а во-вторых, система должна оставить других снаружи. Независимо от того, какая система защиты используется, чаще всего первым шагом работы является идентификация и аутентификация пользователя: кто вы такой и можете ли доказать, что вы это вы?

Идентификация - отождествление, установление соответствия одной сущности другой

Аутентификация - совокупность процедур, цель которых - доказательство того, что идентифицированная сущность является именно той, за которую она себя выдает.

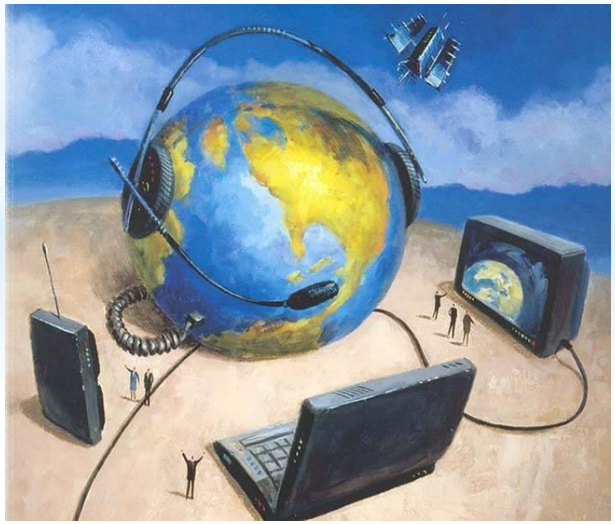
Пользователь идентифицируется именем (идентификатором), а потом аутентифицируется паролем (или другим признаком аутентификации). Как только информационная система (компьютер) узнает вас, он сможет выяснить, что вам разрешено и чего не позволено делать.

Характеристики сравнения биометрических методов анализа

Характеристика	Универсальность	Уникальность	Постоянство	Собираемость
Видеообраз лица	++	+	++	+++
Термограмма лица	+++	+++	+	+++
Отпечаток пальца	++	+++	+++	++
Геометрия руки	++	++	++	+++
Радужная оболочка глаза	+++	+++	+++	++
Сетчатка	+++	+++	++	+
Подпись	+	+	+	+++
Голос	++	+	+	++
Отпечаток губ	+++	+++	++	+
Особенности ушной раковины	++	++	++	++
Динамика письма	+++	+++	+	+++
Походка	+++	++	+	+

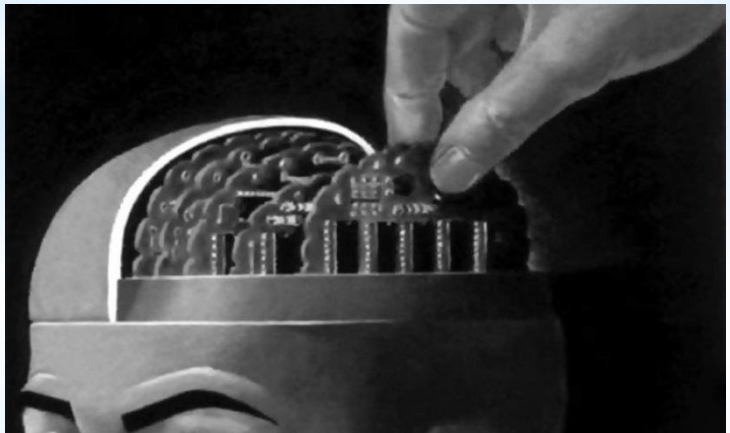
Информационная война

Информационная война - это комплекс мероприятий по достижению информационного превосходства путем воздействия на информацию, информационные процессы, информационные системы и компьютерные сети противника при одновременной защите своей информации, информационных процессов, информационных систем и *компьютерных сетей.*



Военные определяют три **цели** информационной войны:

- контроль информационного пространства, чтобы мы могли использовать его, защищая при этом наши военные информационные функции от вражеских действий (контринформация);
- использование контроля за информацией для ведения информационных атак на врага;
- повышение общей эффективности вооруженных сил с помощью повсеместного использования военных информационных функций.



Наиболее известным примером информационной войны считается холодная война 1946—1991 годов (точнее, её идеологический аспект). Часть исследователей считает, что распад СССР был обусловлен применением информационных методов.

В приведенном примере, **информационная война** – *комплекс мероприятий по информационному воздействию на массовое сознание для изменения поведения людей и навязывания им целей, которые не входят в число их интересов, а также защита от подобных воздействий.*

Холодная война - глобальная геополитическая, экономическая и идеологическая конфронтация между СССР и его союзниками, с одной стороны, и США и их союзниками - *с другой.*

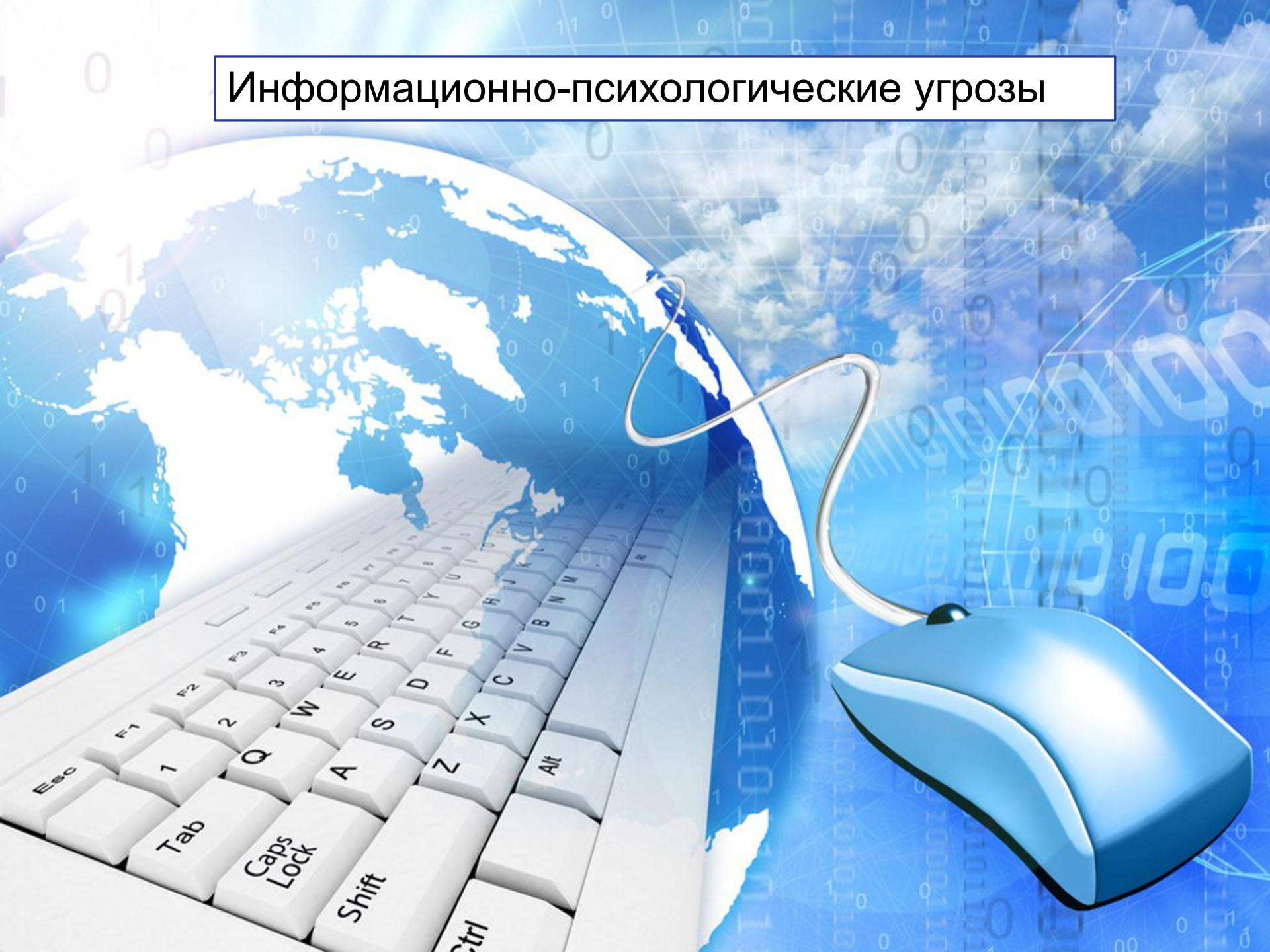
Информационные войны могут вестись:

- между государствами;
- между финансово-промышленными группами;
- между властью и финансово-промышленными группами,
- между властью и оппозицией, которую в свою очередь поддерживают определенные финансово-промышленные группы (иностранные государства);
- между разными сегментами власти, поддерживающие различные финансово-промышленные группы (иностранные государства).

Информационное оружие

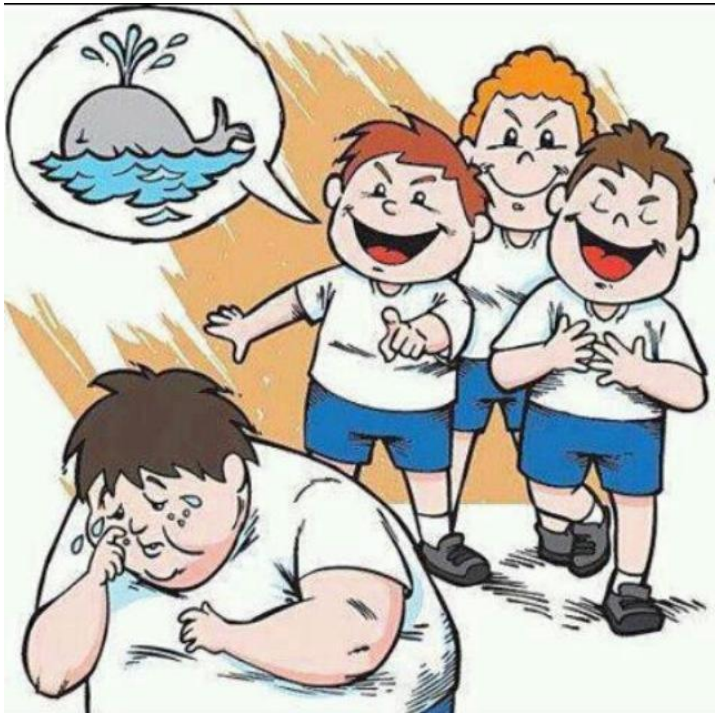
- это комплекс специализированных методов и средств, предназначенных для контроля информационных ресурсов объекта воздействия и временного или безвозвратного вывода из строя функций или служб информационной инфраструктуры в целом или отдельных её элементов.

Информационно-психологические угрозы



БУЛЛИНГ

(от английского **bullying**, bully - хулиган, задира, грубиян) -



это запугивание, психологический или физиологический террор, направленный на подчинение себе другого человека или вызывание у него чувства страха.

КИБЕРБУЛЛИНГ –

одна из форм запугивания, преследования, насилия, травли детей и подростков с помощью информационно-коммуникационных технологий – то есть, мобильных телефонов и интернета.

Круглосуточное вмешательство в личную жизнь

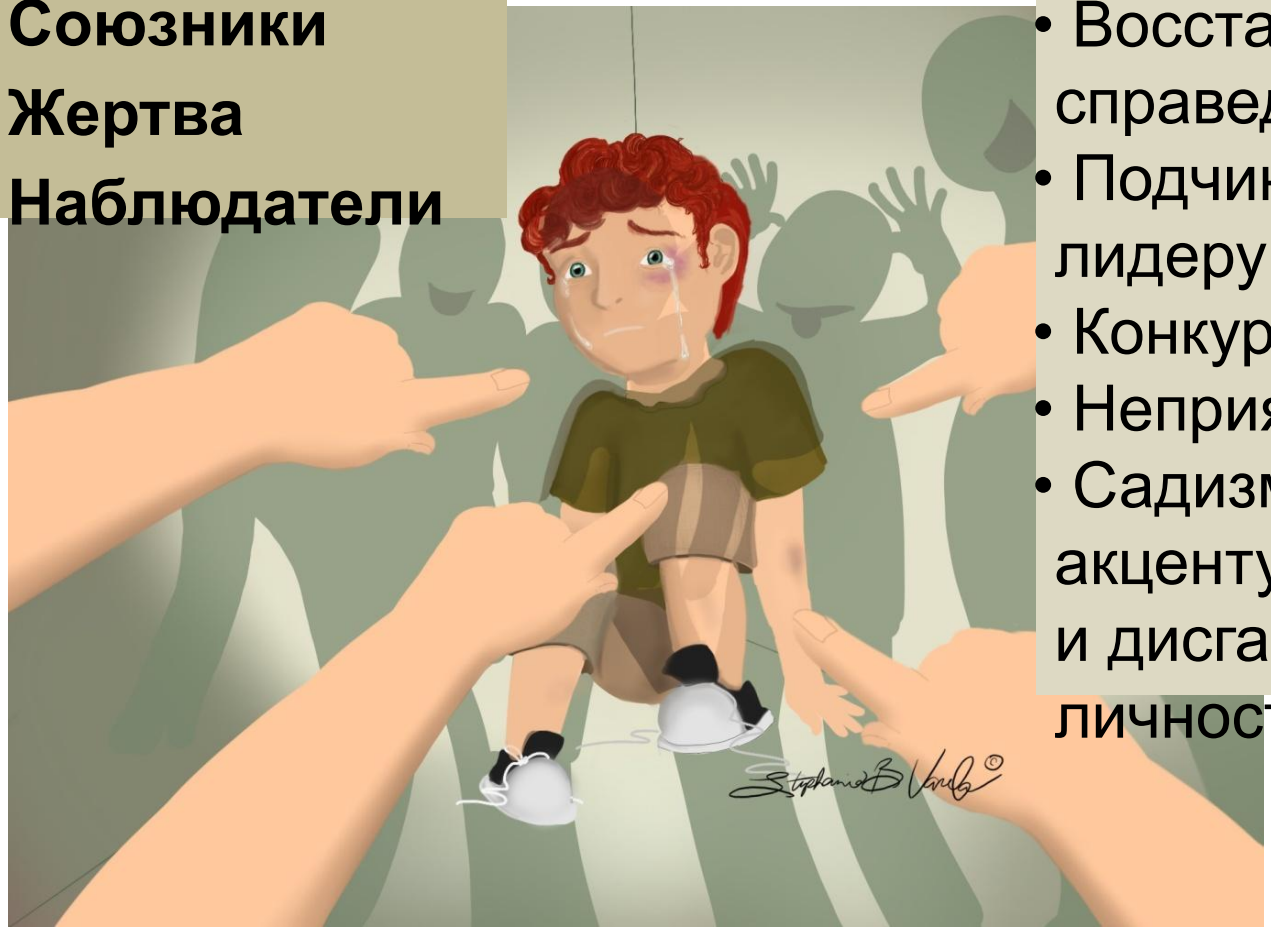
- Травля не имеет временного или географического ограничения.
- Нападки не заканчивается после школы или рабочего дня.

Помни!
Не очень настойчивого и способного хулигана можно занести в чёрные списки и помечать его сообщения как спам.

- Киберхулиган (моббер) круглосуточно имеет прямой доступ через технические средства к жертве: мобильный телефон или профиль в социальных сетях и электронная почта.
- Благодаря постоянным номерам и учётным записям жертва не защищена от нападок и дома.

СОЦИАЛЬНАЯ СТРУКТУРА БУЛЛИНГА

- **Преследователь**
- **Союзники**
- **Жертва**
- **Наблюдатели**



МОТИВАЦИЯ:

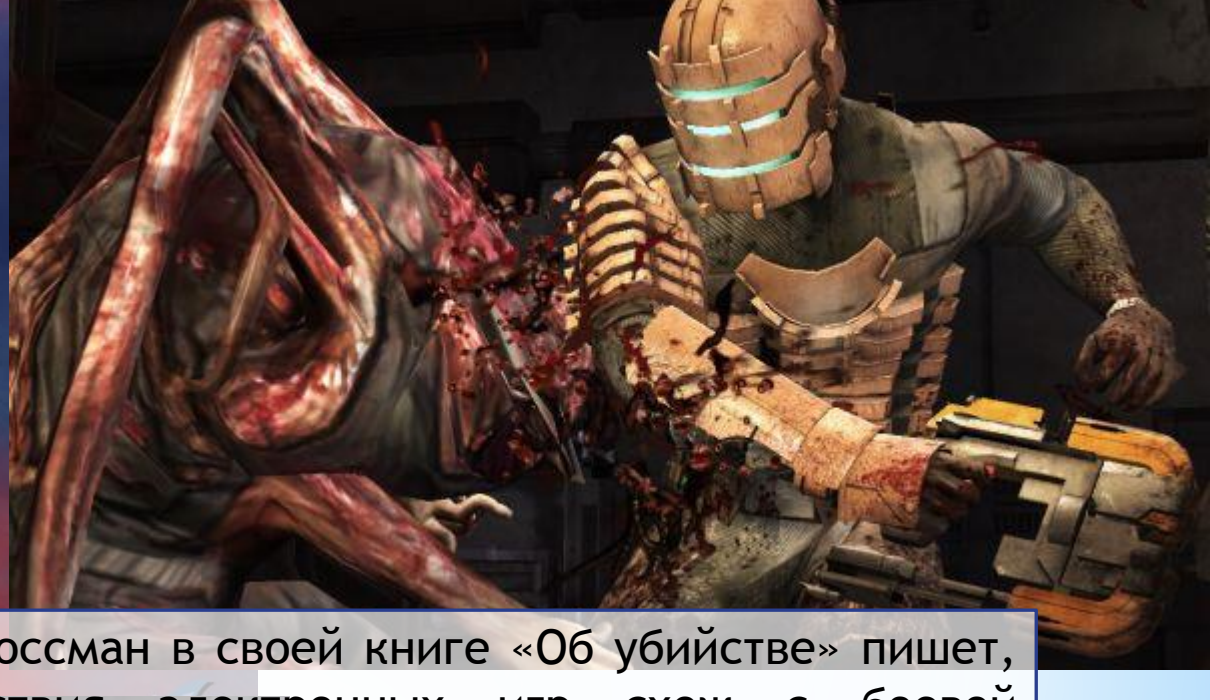
- Месть
- Восстановление справедливости
- Подчинение лидеру
- Конкуренция
- Неприязнь
- Садизм акцентуированных и дисгармоничных личностей

В Москве существует бесплатная служба телефонного и онлайн консультирования для детей и взрослых по проблемам безопасного использования интернета **«Дети онлайн»** — 8-800-25-000-15 с 9 до 18 МСК по рабочим дням.

На Линии помощи профессиональную психологическую и информационную поддержку оказывают психологи факультета психологии МГУ имени М. В. Ломоносова и Фонда Развития Интернет.

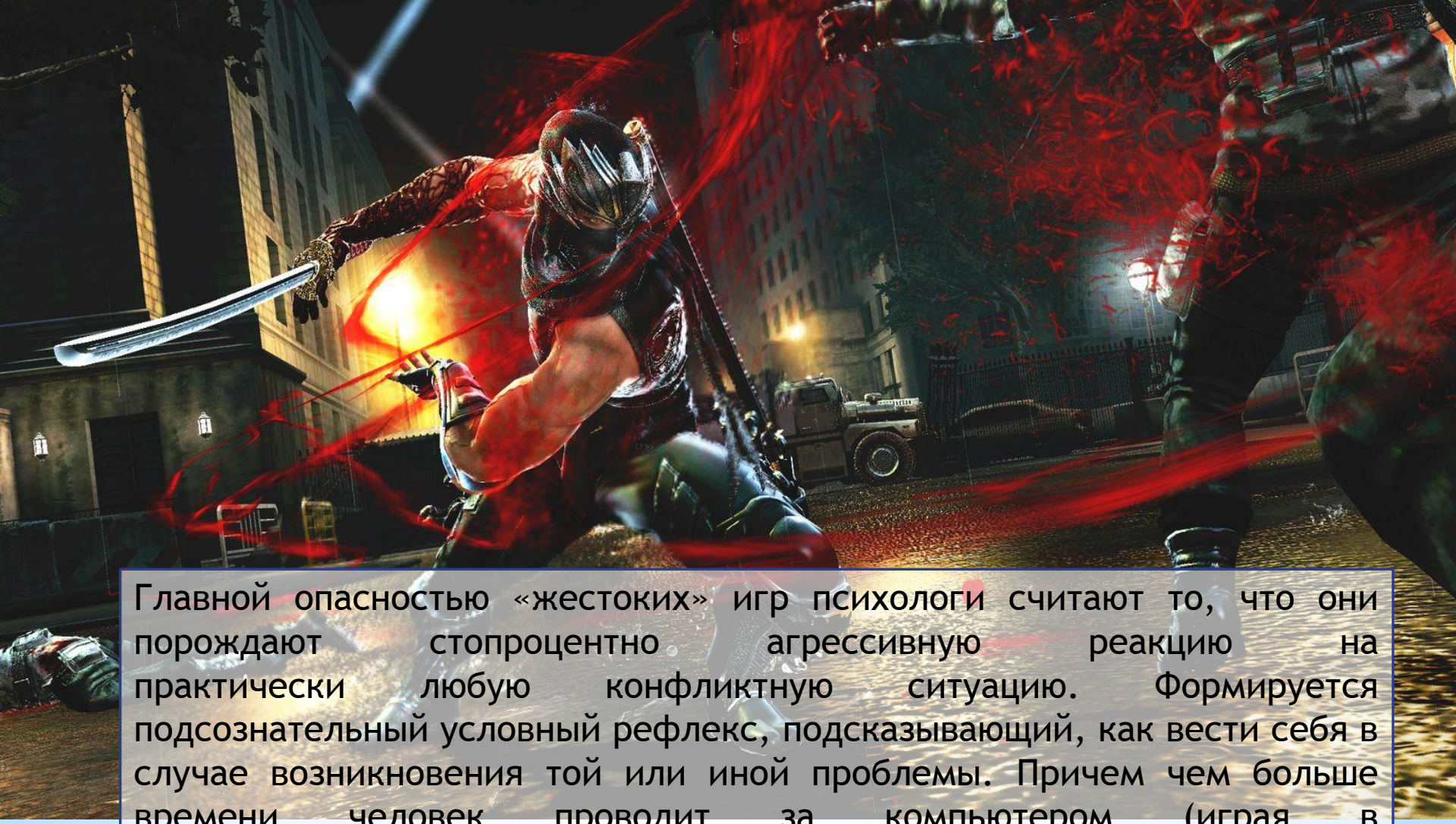
- Также существует группа в социальной сети Вконтакте.ру «Анти-КиберМоббинг» (Anticybermobbing). В которой можно получить консультацию в реальном времени.

Влияние жестоких компьютерных игр на поведение человека

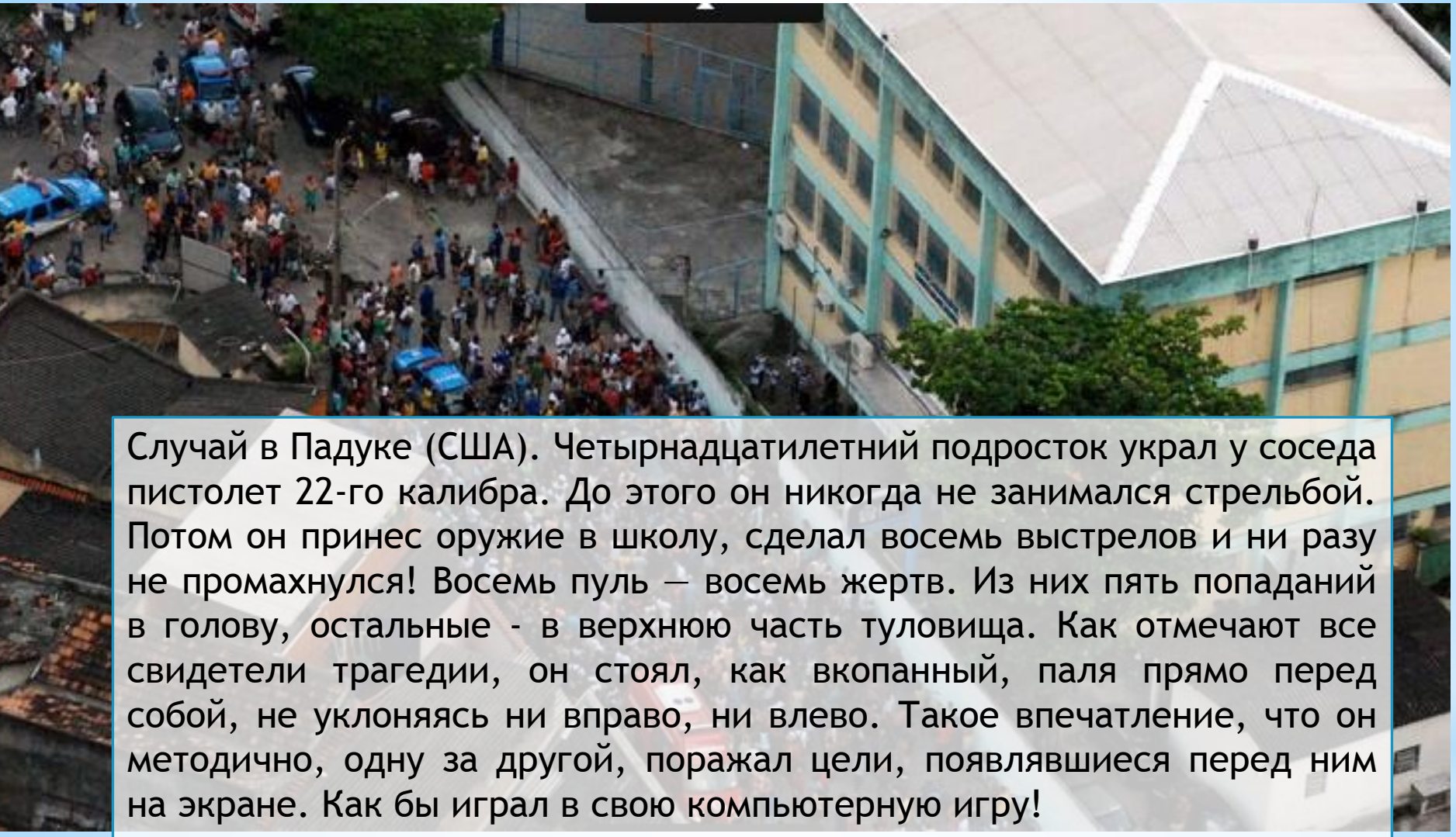


Военный психолог Д. Гроссман в своей книге «Об убийстве» пишет, что механизм воздействия электронных игр схож с боевой подготовкой, во время которой солдаты учатся преодолевать врожденный барьер перед совершением убийства

Четыре национальных организации здравоохранения США выпустили документ, в котором утверждают, что виртуальное насилие напрямую связано с реальным. По мнению ученых, чья работа продолжалось около 9 месяцев и содержит в себе около 1000 отчетов, исследований и т.д., «виртуальное насилие может вызвать у человека агрессивное отношение, поведение, а также просто увеличить агрессивность». Игры делают насилие «привлекательной и обыденной» вещью.



Главной опасностью «жестоких» игр психологи считают то, что они порождают стопроцентно агрессивную реакцию на практически любую конфликтную ситуацию. Формируется подсознательный условный рефлекс, подсказывающий, как вести себя в случае возникновения той или иной проблемы. Причем чем больше времени человек проводит за компьютером (играя в «жестокие» игры), тем выше вероятность того, что любая, даже просто неоднозначная ситуация, требующая анализа и размышлений, будет воспринята им как конфликтная, которую он будет решать единственным доступным ему способом, а именно — силой



Случай в Падуке (США). Четырнадцатилетний подросток украл у соседа пистолет 22-го калибра. До этого он никогда не занимался стрельбой. Потом он принес оружие в школу, сделал восемь выстрелов и ни разу не промахнулся! Восемь пуль — восемь жертв. Из них пять попаданий в голову, остальные - в верхнюю часть туловища. Как отмечают все свидетели трагедии, он стоял, как вкопанный, паля прямо перед собой, не уклоняясь ни вправо, ни влево. Такое впечатление, что он методично, одну за другой, поражал цели, появлявшиеся перед ним на экране. Как бы играл в свою компьютерную игру!

К сведению, для среднестатистического офицера полиции нормальным считается, когда из пяти пуль в цель попадает одна.